Docket No. 243004US2/ims

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Atsuhisa SAITOH, et al. GAU: 2131

SERIAL NO: 10/665,484 EXAMINER:

FILED: September 22, 2003

FOR: IMAGE FORMING DEVICE CONTROLLING OPERATION ACCORDING TO DOCUMENT SECURITY POLICY

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
JAPAN	2002-273985	September 19, 2002
JAPAN	2002-275973	September 20, 2002
JAPAN	2002-297888	October 10, 2002
JAPAN	2002-341222	November 25, 2002
JAPAN	2003-314463	September 5, 2003
JAPAN	2003-314464	September 5, 2003
JAPAN	2003-314465	September 5, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Joseph A. Scafetta Jr.

Marvin J. Spivak
Registration No. 24,913

Joseph A. Scafetta, Jr.
Registration No. 26, 803

Customer Number
22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　９月１９日

出願番号
Application Number: 特願２００２－２７３９８５

[ST. 10/C]: [ＪＰ２００２－２７３９８５]

出願人
Applicant(s): 株式会社リコー

２００３年　７月１８日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５７７２９

【書類名】　特許願
【整理番号】　0201604
【提出日】　平成14年 9月19日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　G06F 15/00
【発明の名称】　複写方法、プログラム、記録媒体、伝送装置及び複写装置
【請求項の数】　15
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　斉藤　敦久
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　金井　洋一
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　谷内田　益義
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　複写方法、プログラム、記録媒体、伝送装置及び複写装置

【特許請求の範囲】

【請求項１】　複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とする複写方法。

【請求項２】　更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手順を有し、

上記判断手順は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手順により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断することを特徴とする請求項１記載の複写方法。

【請求項３】　上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むことを特徴とする請求項１又は２記載の複写方法。

【請求項４】　上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むことを特徴とする請求項１乃至３いずれか一項記載の複写方法。

【請求項５】　上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むことを特徴とする請求項１乃至４いずれか一項記載の複写方法。

【請求項６】　上記セキュリティポリシーは、上記ユーザーにより複写が指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの時

刻とを履歴情報として格納する要件を含むことを特徴とする請求項１乃至５いずれか一項記載の複写方法。

【請求項７】　複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法における処理をコンピューターに実行させるためのプログラムであって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とするプログラム。

【請求項８】　複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法におけるコンピューターに実行させるためのプログラムを格納した記録媒体であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有することを特徴とする記録媒体。

【請求項９】　複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行うプログラムをネットワークを介して伝送する伝送装置であって、

複写する情報を読み取る読取手順と、

上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が

複写可能であるか否かを判断する判断手順と、

上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを他の情報システムに伝送する伝送手順とを有することを特徴とする伝送装置。

【請求項１０】複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写装置であって、

複写する情報を読み取る読取手段と、

上記読取手段により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手段と、

上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手段と、

上記判断手段の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手段とを有することを特徴とする複写装置。

【請求項１１】　更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手段を有し、

上記判断手段は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手段により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断することを特徴とする請求項１０記載の複写装置。

【請求項１２】　上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むことを特徴とする請求項１０又は１１記載の複写装置。

【請求項１３】　上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むことを特徴とする請求項１０乃至１２いずれか一項記載の複写装置。

【請求項１４】　上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むことを特徴とする請求項１０乃至１３いずれか一項記載の複写装置。

【請求項１５】　上記セキュリティポリシーは、上記ユーザーにより複写が

指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの時刻とを履歴情報として格納する要件を含むことを特徴とする請求項１０乃至１４いずれか一項記載の複写装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、複写方法に係り、特に、文書に関するセキュリティポリシーに基づいて複写処理を制御する複写方法に関する。

【０００２】

また、本発明は、そのような複写方法におけるプログラム、及びそのプログラムを格納した記録媒体、ネットワークを介してそのプログラムを伝送するための伝送装置及びその複写方法における処理を行う複写装置に関する。

【０００３】

【従来の技術】

近年、多くのオフィス業務では、ファックス、プリンター、複写機などの情報システムを用いて文書が扱われている。このような情報システムに依存して日常の業務が行われるにつれて、その文書を扱う情報システムのセキュリティ確保が重要視されるようになってきている。特に、最近では官公庁を中心としてＩＳＯ１７７９９として知られる情報セキュリティ管理標準に基づいて組織の情報セキュリティポリシーを掲げるところが増え、そのポリシーに基づいてセキュリティを確保した情報システムの構築・運営が行われている。このような動向は、官公庁から自治体、そして取引先である大手企業に広がる傾向にあり、大手企業の取引先である中小企業へとその動きが広がっていくことが容易に予想できる。この動向そのものは、健全な情報システムの構築を加速させるものとして歓迎すべきである。

【０００４】

また、上記のような情報システムに設定するセキュリティポリシー（通常ポリシーファイルという形式で設定される）には、例えば、Ｊａｖａ（登録商標）に設定するプログラムの実行許諾に関する設定情報や、ファイアウォールに設定す

るプロトコルの通過許可に関する設定情報などがある。

【０００５】

一般に、情報システムのセキュリティの確保は、機密性、完全性、可用性の確保に大別される。完全性や可用性は情報システムの管理者が適切に運営・管理すれば、実質上問題のないレベルを確保できる場合が多い。一方、機密性の確保のためには、中小企業に代表される情報システムのユーザー組織に所属するユーザーのそれぞれにセキュリティポリシーを共有・徹底させなければならない。このような理由で、特に、情報システムのコンテナである文書に対するポリシー、中でも機密保持に関するポリシーが重要視されているため、多くの企業では、文書に関するセキュリティを制御する要求が高まっている。

【０００６】

例えば、従来技術として、データファイルへのアクセスに対応するポリシーの評価を行う手段に加えて、ポリシーに条件が記述してあり、その条件をクリアにするための執行手段がある場合には、それを執行することでアクセス許可の評価を行っている（例えば、特許文献１参照）。しかしながら、データファイルへのアクセス制御システムであって、アクセス後のデータの処理、特に複写などには言及されていない。

【０００７】

また、従来技術として、ポリシー、システム、制御手段で構成され、それぞれの組み合わせが登録されたＤＢから制御手段を抽出して、システムをポリシーに合うように制御する手段と、その状態を監査する手段とを有する（例えば、特許文献２参照）。しかしながら、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低いという問題がある。

【０００８】

また、従来技術として、ファイルへのアクセス制御をポリシーファイル（記述を列挙してある）に基づいて行い、単一システムによる制御及び制御部を分離したもの、複数のＯＳによる制御、サーバクライアントプロセスによる制御などを行っている（例えば、特許文献３参照）。

【０００９】

また、従来技術として、第三者機関にセキュリティポリシーを設定、更新し、ネットワークを介してアクセス制御を行い、セキュリティ侵害の収集、解析、警告、否認不可保証を行い、異なるネットワークのオブジェクトを関連付けて、他のネットワークへのアクセスを管理し、関連付けられたオブジェクトの不整合を調整し、セキュリティポリシーに従って動作する機能のＡＰＩ（Ａｐｐｌｉｃａｔｉｏｎ　Ｐｒｏｇｕｒａｍ　Ｉｎｔｅｒｆａｃｅ）を提供する（例えば、特許文献４参照）。

【００１０】

また、従来技術として、ユーザーの証明書の確認を行うか否かをセキュリティポリシーに記述し、確認の方法には、唯一のユーザを特定できる高レベル、クライアントの認証結果を利用する中レベル、利用するプロトコルから判断する低レベルの３レベルがあり、低レベルで確認されたユーザは高いレベルで確認されたユーザのジョブに対してオペレーションできないなどのオペレーションの制御を行っている（例えば、特許文献５参照）。

【００１１】

また、従来技術として、セキュリティ管理者はユーザー、グループをサイト（プリンタ）のセキュリティレベルに応じてセキュリティ管理を行い、サイト（プリンタ）管理者はプリンタのジョブの実行制限を行い、ユーザはパスワードなしで自分のファイルを表示印刷される場合に「禁止」などのラベルを付加できる（例えば、特許文献６参照）。

【００１２】

【特許文献１】

特開２００１－１８４２６４号公報

【特許文献２】

特開２００１－２７３３８８号公報

【特許文献３】

特開２００１－３３７８６４号公報

【特許文献４】

特開平７－１４１２９６号公報

【特許文献５】

特開平９－２９３０３６号公報

【特許文献６】

特許第２７３５９６６号明細書。

【００１３】

【発明が解決しようとする課題】

上記のように現在、多くの企業ではセキュリティポリシーを設け、そのセキュリティポリシーを制御しようとしているが、実際、オフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティポリシーではなく、オフィスシステムを構成するさまざまな情報システムに関して、個別にセキュリティ設定を行う必要がある。従って、このようなセキュリティ設定を行うためにさまざまな情報システムに関する知識が必要となってしまうという問題点があった。

【００１４】

また、複数の情報システムの一つ一つにセキュリティポリシーを設定しなければならならず、手間が煩雑になるという問題点があった。

【００１５】

このように従来の複数の情報システムでは個別にセキュリティ設定を行っているため、情報システム全体がどのようなセキュリティ状態になっているかを把握するのが難しいという問題点があった。

【００１６】

一方、従来の複数の情報システムのそれぞれにセキュリティの設定を行うことができても、実際に文書のセキュリティが守られていることをユーザーは明確に認識することができないという問題点があった。

【００１７】

そこで、本発明の課題は、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる複写方法、記録媒体、伝送装置及び複写装置を提供することである。

【００１８】

【課題を解決するための手段】

上記の課題を解決するため、本発明は、複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、複写する情報を読み取る読取手順と、上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有する構成とされる。

【００１９】

このような複写方法では、複写する情報を読み取り、読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得し、文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断し、判断結果に基づいて、読取情報を所定の媒体に印刷させることにより、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【００２０】

複写を指示するユーザーのセキュリティを判断するという観点から、本発明は、請求項２に記載されるように、更に、複写を指示したユーザーに関する情報を取得するユーザー情報取得手順を有し、上記判断手順は、上記文書のセキュリティが所定値以上のとき、上記ユーザー情報取得手順により取得されたユーザー情報と上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断するように構成することができる。

【００２１】

このような複写方法では、更に、複写を指示したユーザーに関する情報を取得し、判断手順は、文書のセキュリティが所定値以上のとき、取得されたユーザー情報と文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断することにより、複写を指示したユーザーによる複写が可能であるかを判断することができる。

【００２２】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項３に記載されるように、上記セキュリティポリシーは、複写する上記読取情報に電子透かしを付加して印刷する要件を含むように構成することができる。

【００２３】

このような複写方法では、セキュリティポリシーは、複写する読取情報に電子透かしを付加して印刷する要件を含むことにより、読取情報に電子透かしを入れて印刷するように複写処理を制御することができる。

【００２４】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項４に記載されるように、上記セキュリティポリシーは、複写する上記読取情報にバーコードを付加して印刷する要件を含むように構成することができる。

【００２５】

このような複写方法では、セキュリティポリシーは、複写する読取情報にバーコードを付加して印刷する要件を含むことにより、読取情報にバーコードを入れて印刷するように複写処理を制御することができる。

【００２６】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項５に記載されるように、上記セキュリティポリシーは、複写する上記読取情報を特定の媒体に印刷する要件を含むように構成することができる。

【００２７】

このような複写方法では、セキュリティポリシーは、複写する読取情報を特定の媒体に印刷する要件を含むことにより、柔軟に文書のオペレーションを制御することができると共に、読取情報を特定の媒体に印刷するように複写処理を制御することができる。

【００２８】

柔軟な要件に応じて読取情報を印刷するという観点から、本発明は、請求項６に記載されるように、上記セキュリティポリシーは、上記ユーザーにより複写が指示されたとき、上記ユーザー情報と、上記読取情報と、複写を指示したときの

時刻とを履歴情報として格納する要件を含むように構成することができる。

【００２９】

このような複写方法では、セキュリティポリシーは、ユーザーにより複写が指示されたとき、ユーザー情報と、読取情報と、複写を指示したときの時刻とを履歴情報として格納する要件を含むことにより、ユーザーは読取情報のセキュリティ状態や、複写処理の印刷状態を把握することができる。

【００３０】

また、上記課題を解決するため、本発明は、上記複写方法における処理をコンピューターに実行させるプログラム、そのプログラムを格納した記録媒体、ネットワークを介して複写方法における処理を伝送するための伝送装置、及び複写装置とすることもできる。

【００３１】

【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて説明する。本発明の実施の一形態に係る複写方法は、複写装置において、文書に関して生成されたセキュリティポリシーに基づいて複写処理を制御する。その複写装置のハードウェア構成は、例えば、図１に示すようになっている。

【００３２】

図１は、本発明の実施の一形態に係る複写装置のハードウェア構成を示すブロック図である。

【００３３】

図１において、複写装置１０は、ＣＰＵ１１と、ＲＯＭ１２と、ＲＡＭ１３と、ＨＤＤ１４と、スキャナ１５と、プロッタ１６と、表示操作部１７と、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）１８とで構成される。これらの各ユニットはバス１９を介して接続されている。ＣＰＵ１１は、ＲＯＭ１２に格納された複写装置を制御するためのプログラム、及びＨＤＤ１４からＲＡＭ１３に転送されるプログラムとに基づいて、複写装置１０を制御する。また、ＣＰＵ１１は、ＲＡＭ１３を作業メモリ空間として利用すると共に、ＲＡＭ１３から処理対象のデータを読み出して処理する。処理後のデータはＲＡＭ１３に格納

される。ＨＤＤ１４は、文書ファイル、複写方法に係るプログラムなどを格納する。スキャナ１５は、印刷物をスキャンして電子データとして取り込むスキャナ処理を行う。プロッタ１６は、パーソナルコンピュータ（ＰＣ）などで生成した電子文書を印刷する場合や、印刷物などを複写する印刷処理を行う。ＮＩＣ１８は、ネットワークインターフェースであり、ネットワークと接続されて複数の情報システムとセキュリティポリシーなどの複写方法に関する情報の送受信を行う。表示操作部１７は、オペレーションパネルなどで構成され、ユーザからの入力操作の受け付け並びにユーザに向けた表示を行う。

【００３４】

このようなハードウェア構成を採用することにより、複数の情報システム、特に複写装置１０のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【００３５】

尚、セキュリティポリシー１００を記録する記録媒体は、上記ＲＯＭ１２、ＲＡＭ１３、ＨＤＤ１４に限定されることなく、セキュリティポリシー１００を記録することができ、コンピュータが読み取り可能な媒体であれば適応可能である。

【００３６】

図２は、本発明の実施の一形態に係る複写方法におけるシステム構成図である。図２において、複写方法に係る複写装置１０は、ネットワーク１を介して、他の複写装置、ファックス、プリンタなどの複数の情報システム３０に接続される。複写装置１０は、文書に関するセキュリティポリシー１００と、ユーザーによる複写指示の入力操作並びに複写処理に関する通知が行われるオペレーションパネル２１と、複写する印刷物などから情報を読み取る読み取り処理部２２と、複写を行うユーザーの属性を取得するユーザー属性取得処理部２３と、複写する文書に関する属性を取得する文書属性取得処理部２４と、セキュリティポリシー１００に基づいて印刷処理を行う印刷処理部２５と、読み取り処理部２２により読み取られた情報を格納する読み取り情報ＤＢ２６と、文書の属性情報が格納された文書属性ＤＢ２７と、ユーザーの属性情報が格納されたユーザー属性ＤＢ２８

とで構成される。この複写装置１０は、図１に示すＣＰＵ１１（中央処理装置）によって各構成が制御される。

【００３７】

以下に、複写装置１０で行われる複写処理の手順について説明する。ユーザーにより、複写装置１０のオペレーションパネル２１から複写指示が入力されると、オペレーションパネル２１は、読み取り処理部２２、ユーザー属性取得処理部２３に複写指示を供給する。読み取り処理部２２は、複写指示に応じて印刷物から複写する情報を読み取り、読み取り情報ＤＢ２６に格納する。また、読み取り処理部２２は、文書属性取得処理部２４に読み取り情報を供給する。文書属性取得処理部２４は、読み取り情報に基づいて、文書属性ＤＢ２７に格納された文書属性を取得し、取得した文書属性を読み取り処理部２２及び印刷処理部２５に供給する。読み取り処理部２２及び印刷処理部２５は、文書属性とセキュリティポリシー１００とに基づいて、セキュリティポリシー１００に記述された文書の要件を満たしているかを判断する。

【００３８】

更に、読み取り処理部２２及び印刷処理部２５は、判断結果から必要に応じて、ユーザー属性処理部２３にユーザー属性の要求を供給する。ユーザー属性処理部２３は、オペレーションパネル２１にユーザー情報の入力を促す情報の表示を指示し、ユーザー情報を取得する。ユーザー属性処理部２３は、ユーザー情報に基づいて、ユーザー属性ＤＢ２８に格納されたユーザー属性を読み取り処理部２２及び印刷処理部２５に供給する。読み取り処理部２２及び印刷処理部２５は、ユーザー属性処理部２３からのユーザー属性に基づいて、セキュリティポリシー１００に記述されたユーザーの要件を満たしているかを判断する。印刷処理部２５は、判断結果に応じて読み取り情報を印刷する。読み取り処理部２２は、印刷結果をオペレーションパネル２１に表示する指示を供給する。

【００３９】

尚、複写装置１０は、上記一連の複写処理を実行するためのプログラムを、ネットワーク１を介して情報システム３０に伝送することで、複数の情報システム３０、特に、他の複写装置のセキュリティポリシーを共有させることができる。

従って、複数の情報システムのセキュリティポリシーを統括して管理することが可能となる。

【００４０】

次に、文書に関するセキュリティポリシー１００の記述について説明する。尚、セキュリティポリシー１００は、ＸＭＬ（ｅＸｔｅｎｓｉｂｌｅ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式で記述するものとする。図３は、文書に関するセキュリティポリシーの例を示す図である。図３において、セキュリティポリシー１００には、記述１２０と記述１２１に示す＜policy＞と＜/policy＞とで囲まれた範囲の記述１０１～１１０、１２２、１２３に、文書に関するセキュリティポリシーの要件が設定されている。記述１２０には、セキュリティポリシー１００を識別するための情報が記述されている。記述１２２、１２３に示す＜ace_rule＞は、文書に対して許可される操作（オペレーション）や、ユーザーに対するオペレーションの許可に関する要件が設定されている。

【００４１】

まず、記述１２２の要件について説明する。

【００４２】

記述１０１示す文書のカテゴリ＜doc_category＞には、どの文書のカテゴリにも適応する「ＡＮＹ」が設定されている。記述１０２に示す文書のセキュリティレベル＜doc_security_level＞には、文書のセキュリティレベルが標準であることを示す「basic」が設定されている。記述１０３に示すユーザーのカテゴリ＜user_category＞には、どのユーザーのカテゴリにも適応する「ＡＮＹ」が設定されている。記述１０４に示すユーザーのセキュリティレベル＜user_security_level＞には、どのユーザーにも適応する「ＡＮＹ」が設定されている。記述１０５に示す＜name＞hardcopy＜/name＞＜allowed/＞は、複写処理を要件なく許可することを示している。

【００４３】

次に、記述１２３の要件について説明する。

【００４４】

記述１０６示す文書のカテゴリ＜doc_category＞には、どの文書のカテゴリに

も適応する「ＡＮＹ」が設定されている。記述１０７に示す文書のセキュリティレベル＜doc_security_level＞には、文書のセキュリティレベルの高いことを示す「high」が設定されている。記述１０８に示すユーザーのカテゴリ＜user_category＞には、ユーザーのカテゴリと文書のカテゴリが同等であることを示す「ＤＯＣ－ＣＡＴＥＧＯＲＹ」が設定されている。記述１０９に示すユーザーのセキュリティレベル＜user_security_level＞には、どのユーザーにも適応する「ＡＮＹ」が設定されている。記述１１０に示す＜name＞hardcopy＜/name＞＜requirement＞audit＜/requirement＞＜requirement＞embed_trace_info＜/requirement＞は、複写処理において、印刷履歴情報を記録する要件と、追跡可能な情報を埋め込む要件を満たすときに許可することを示している。

【００４５】

このように、複写装置１０は、要件が設定されたセキュリティポリシー１００に基づいて複写処理を行うことにより、文書及びユーザーのセキュリティの要件を満たした複写処理を行うことができる。また、セキュリティポリシー１００がＸＭＬ形式で記述されていることにより、プラットホームに依存せずに情報システム３０全体にセキュリティポリシーを共有させることができる。

【００４６】

尚、上記印刷履歴情報を記録する要件において、ユーザーによりオペレーションパネル２１から複写が指示されたときにユーザー情報、読取情報、複写を指示したときの時刻などを記録するように設定してもよい。

【００４７】

次に、上記複写装置１０で実行される複写処理の手順について説明する。図４は、複写処理を説明するためのフローチャート図である。図４において、先ず、ステップＳ１０の処理で、ユーザーにより複写装置１０に紙文書が読み取り処理部２２にセットされた状態で、オペレーションパネル２１に複写指示が入力されると、オペレーションパネル２１から読み取り処理部２２及びユーザー属性取得処理部２３に複写指示が供給される。ステップＳ１１の処理で、読み取り処理部２２は、紙文書から複写する情報を読み取り、読み取り情報ＤＢ２６に読み取り情報を格納すると共に、印刷処理部２５及び文書属性取得処理部２４に読み取り

情報を供給する。ステップＳ１２の処理で、文書属性取得処理部２４は、読み取り情報に基づいて、文書属性ＤＢ２７に格納された文書属性を取得し、読み取り処理部２２及び印刷処理部２５に供給する。尚、文書属性取得処理部２４は、読み取り情報のバーコードや、電子透かし等の画像情報から文書のＩＤを抽出して、文書属性ＤＢ２７に格納された文書属性を取得するようにしてもよい。

【００４８】

ステップＳ１３の処理で、読み取り処理部２２及び印刷処理部２５は、セキュリティポリシー１００及び文書属性とに基づいて、その文書の複写に対する要件が有るか否かを判断する。例えば、ステップＳ１２の処理において、複写する文書情報のセキュリティレベルが、図２に示すセキュリティポリシー１００に設定されている、文書のセキュリティレベル「basic」の場合、要件がないものと判断される。また、複写する文書情報のセキュリティレベルが、文書のセキュリティレベル「high」の場合、印刷履歴情報を記録する要件と、追跡可能な情報を埋め込む要件があるものと判断される。

【００４９】

ステップＳ１３の処理で、その文書の複写に対する要件が有る場合、ステップＳ１４の処理で、読み取り処理部２２及び印刷処理部２５は、その要件全てを満たすか否かを判断する。ステップＳ１４の処理で、その要件全てを満たさない場合、ステップＳ１６の処理で、読み取り処理部２２及び印刷処理部２５は、読み取った文書情報を破棄して印刷を中止すると共に、ユーザーに通知するためにオペレーションパネル２１に印刷中止の情報を供給する。ステップＳ１４の処理で、その要件全てを満たす場合、ステップＳ１７の処理で、読み取り処理部２２及び印刷処理部２５は、読み取った文書情報を印刷する。例えば、ステップＳ１７の処理は、複写する文書情報のセキュリティレベルが、図２に示すセキュリティポリシー１００に設定されている、文書のセキュリティレベル「high」の場合に実行される。具体的には、第１に、ユーザー属性取得処理部２３は、オペレーションパネル２１から複写指示を出したユーザーにユーザーＩＤの入力を促す情報の表示を指示する。第２に、ユーザーは、オペレーションパネル２１からユーザーＩＤを入力する。第３に、ユーザー属性取得処理部２３は、ユーザーＩＤに基

づいて、ユーザー属性ＤＢ２８に格納されているユーザー属性から入力されたユーザーＩＤに対応するカテゴリー、セキュリティレベルを取得し、読み取り処理部２２と印刷処理部２５とに供給する。第４に、読み取り処理部２２又は印刷処理部２５のどちらか一方が、印刷履歴情報を記録する。第５に、印刷処理部２５は、追跡可能な情報の埋め込み、例えば、電子透かし、バーコードなどを追加して印刷を行い、複写処理を終了する。

【００５０】

一方、ステップＳ１３の処理で、その文書の複写に対する要件がない場合、ステップＳ１５の処理で、印刷処理部２５は、読み取った文書情報を印刷し、複写処理を終了する。例えば、ステップＳ１３の処理は、複写する文書情報のセキュリティレベルが、図２に示すセキュリティポリシー１００に設定されている、文書のセキュリティレベル「basic」の場合に実行される。

【００５１】

このように、上記複写方法において、ユーザーによりオペレーションパネル２１から複写指示があると、読取処理部２２により複写する情報を読み取り、文書属性取得処理部２４により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性を取得し、読取処理部２２、印刷処理部２５により文書属性とセキュリティポリシー１００とに基づいて、読取情報が複写可能であるか否かを判断して読取情報を印刷することにより、そのセキュリティポリシー１００を反映させた複写処理を行うことができる。更に、ユーザー属性取得処理部２３により複写を指示したユーザーに関する情報を取得し、読取処理部２２、印刷処理部２５によりユーザー属性情報と文書属性とセキュリティポリシー１００とに基づいて、読取情報が複写可能であるか否かを判断することにより、複写を指示したユーザーによる複写が可能であるかを判断することができる。

【００５２】

また、上記複写方法における処理を、複数の情報システムに伝送することにより、特に複数の複写装置に共通のセキュリティポリシー１００を統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる

尚、上記複写処理において読み取られた紙文書の情報を複写する媒体は、紙に

限定されることなく、ＯＣＲ用の特定の印刷用紙などにも適応可能である。

【００５３】

【発明の効果】

上述の如く本発明によれば、複写する情報を読み取り、読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得し、文書属性情報とセキュリティポリシーとに基づいて、読取情報が複写可能であるか否かを判断し、判断結果に基づいて、読取情報を所定の媒体に印刷させることにより、複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる。

【図面の簡単な説明】

【図１】

本発明の実施の一形態に係る複写装置のハードウェア構成を示すブロック図である。

【図２】

本発明の実施の一形態に係る複写方法におけるシステム構成図である。

【図３】

文書に関するセキュリティポリシーの例を示す図である。

【図４】

複写処理を説明するためのフローチャート図である。

【符号の説明】

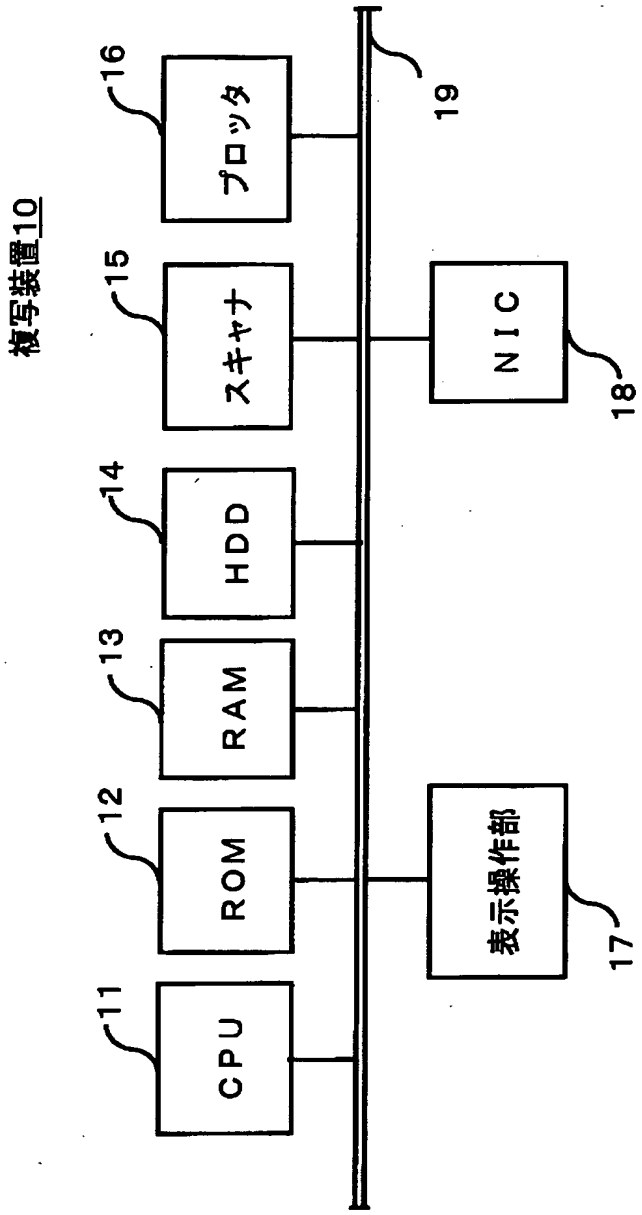
１	ネットワーク
１０	複写装置
１１	ＣＰＵ
１２	ＲＯＭ
１３	ＲＡＭ
１４	ＨＤＤ
１５	スキャナ
１６	プロッタ
１７	表示操作部

１８	ＮＩＣ
１９	バス
２１	オペレーションパネル
２２	読み取り処理部
２３	ユーザー属性取得処理部
２４	文書属性取得処理部
２５	印刷処理部
２６	読み取り情報ＤＢ
２７	文書属性ＤＢ
２８	ユーザー属性ＤＢ
３０	情報システム
１００	セキュリティポリシー

【書類名】　図面

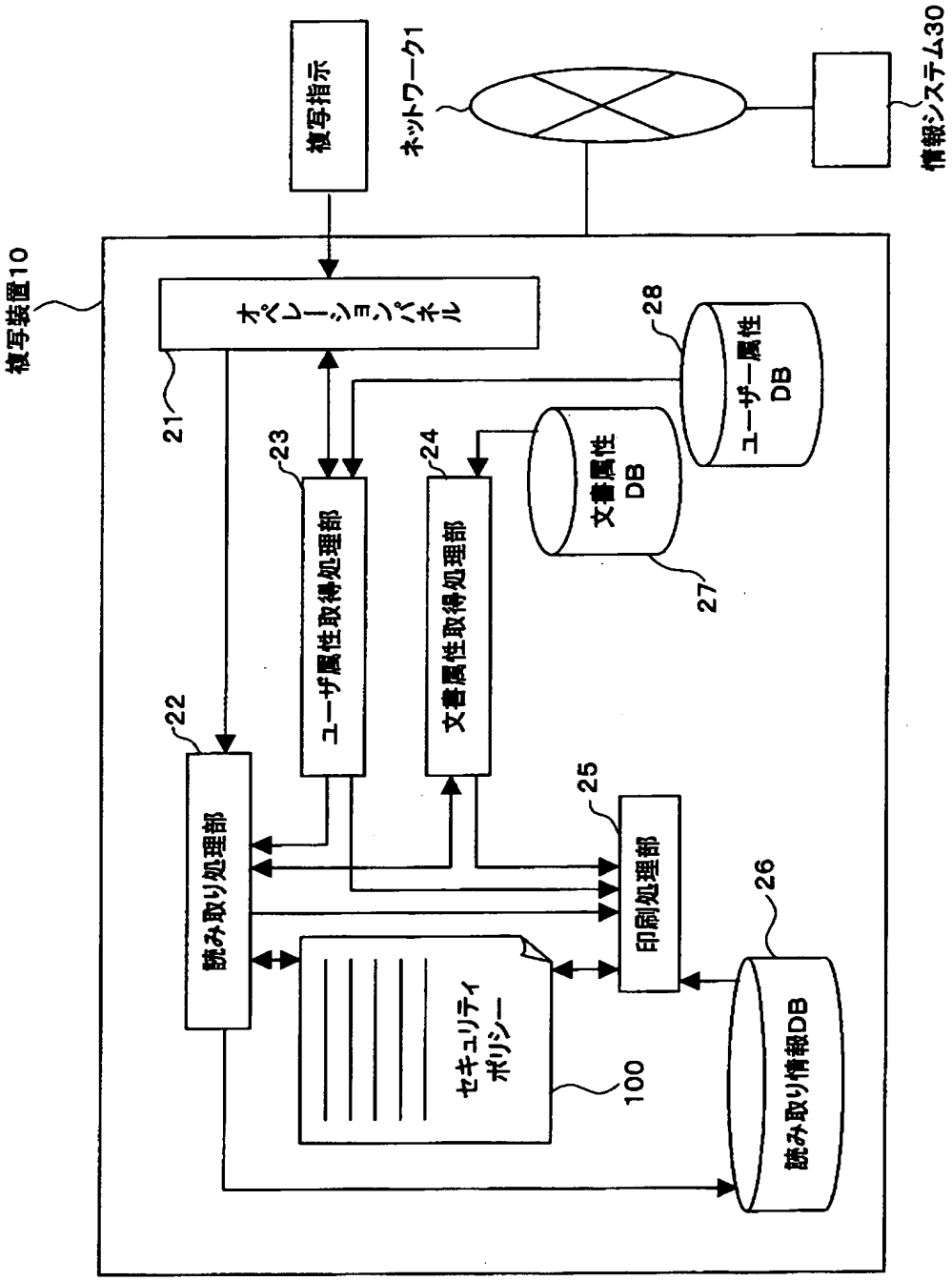
【図１】

本発明の実施の一形態に係る複写装置のハードウェア構成を示すブロック図



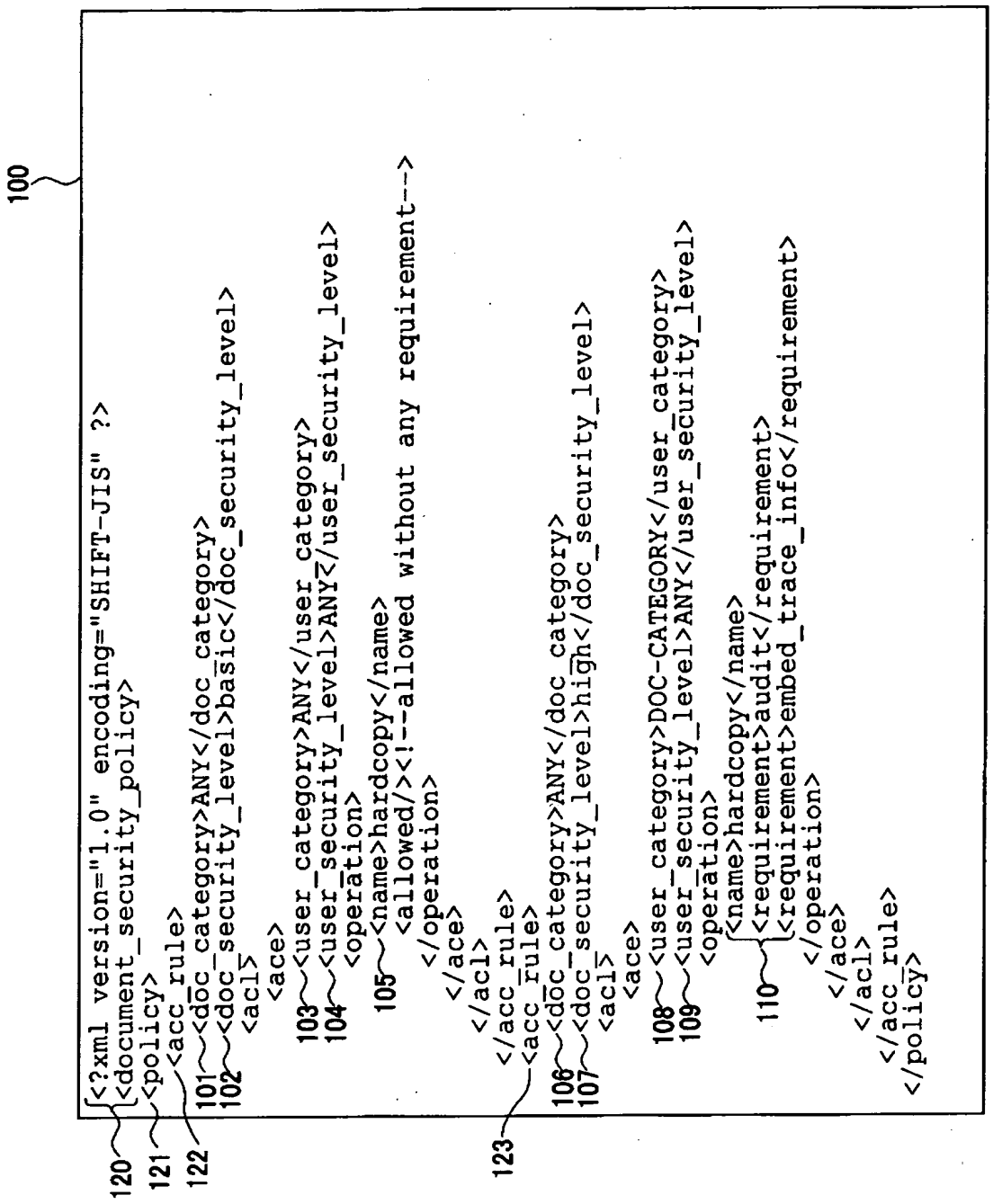
【図２】

本発明の実施の一形態に係る複写方法における
システム構成図



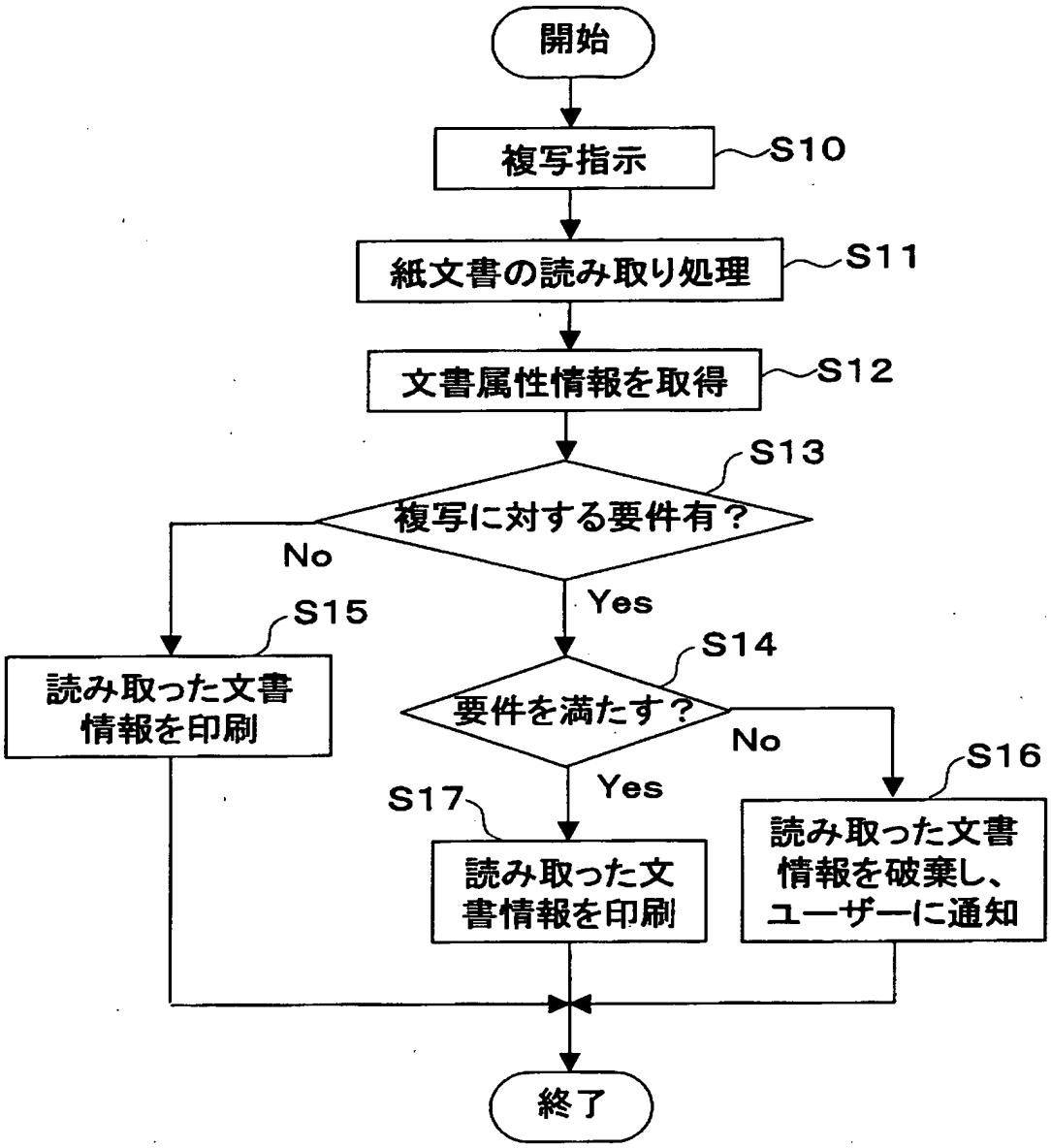
【図３】

文書に関するセキュリティポリシーの例を示す図



【図４】

複写処理を説明するためのフローチャート図



【書類名】　　要約書

【要約】

【課題】　複数の情報システム、特に複写装置のセキュリティポリシーを統括して管理し、そのセキュリティポリシーを反映させた複写処理を行うことができる複写方法を提供することを目的とする。

【解決手段】　本発明の課題は、複写を実行する要件を有するセキュリティポリシーに基づいて複写処理を行う複写方法であって、複写する情報を読み取る読取手順と、上記読取手順により読み取られた読取情報に基づいて、文書のセキュリティに関する文書属性情報を取得する属性情報取得手順と、上記文書属性情報と上記セキュリティポリシーとに基づいて、上記読取情報が複写可能であるか否かを判断する判断手順と、上記判断手順の判断結果に基づいて、上記読取情報を所定の媒体に印刷させる印刷手順とを有する構成とされる。

【選択図】　　図２

特願２００２－２７３９８５

出　願　人　履　歴　情　報

識別番号　　［０００００６７４７］

１．変更年月日　　１９９０年　８月２４日
［変更理由］　　新規登録
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー

２．変更年月日　　２００２年　５月１７日
［変更理由］　　住所変更
住　所　　東京都大田区中馬込１丁目３番６号
氏　名　　株式会社リコー